BY ORDER OF THE COMMANDER
AIR MOBILITY COMMAND

AIR MOBILITY COMMAND INSTRUCTION
24-101 VOLUME 4

21 APRIL 2011

Transportation

MILITARY AIRLIFT/AIR TRANSPORTATION SYSTEMS MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-publishing.af.mil** for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: HQ AMC/A4T

Certified by: HQ AMC/A4T
(Col William Z. Zeck)

Supersedes: AMCI 24-101V4, 9 April 2008

Pages: 29

This volume describes automation and communication procedures for developing, operating, and managing the Air Mobility Command (AMC) transportation computer systems used to control and record the movement of passengers, cargo, and mail for all AMC aerial ports and air terminals. It also provides guidance for those non-AMC organizations which are using AMC automated systems. This volume applies to Air Force Reserve Command (AFRC) units but not Air National Guard (ANG) units. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional chain of command to HQ AMC A4TI at **amc.a4ti@scott.af.mil.** Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at **https://www.my.af.mil/afrims/afrims/afrims/rims.cfm**. See Attachment 1 for a glossary of references and supporting information.

SUMMARY OF CHANGES

This document has been substantially revised and must be completely reviewed. Major changes includes updated office symbols and internet links, added responsibilities, new guidance on the Global Air Transportation Execution System (GATES) password management and user authentication procedures, changed the term GATES TMO to Passenger Reservations and provided enhanced guidance on the GATES access process.

1. General.

1.1. Three separate functional community requirements are now integrated into GATES: AMC and aerial port operations, United States Transportation Command (USTRANSCOM) with the Defense Courier Service (DCS), and the Surface Deployment and Distribution Command (SDDC) with the Worldwide Port System. As a joint system, GATES is managed by USTRANSCOM. This instruction only applies to GATES as it pertains to AMC's aerial port operations and air transportation.

1.2. AMC must provide automation support and data capture of aerial port transportation activities to meet wartime mission requirements as well as sustain normal peacetime operations. Automation is required to support aerial port operations and AMC financial management obligations, as well as to provide In-Transit Visibility (ITV) for cargo and passengers moving on AMC airlift.

2. Responsibilities:

2.1. **Headquarters (HQ) AMC/A4T will:**

2.1.1. Provide policy guidance on Aerial Port Operations.

2.1.2. Coordinate transportation systems development and planning with HQ AMC/A4TI.

2.1.3. Coordinate policy changes that affect transportation automation systems with HQ AMC/A4TI.

2.1.4. Review system metrics and identify problem areas that impact efficient operation of transportation automation systems and take appropriate action to facilitate correction.

2.1.5. Serve as a voting member on the USTRANSCOM Joint Functional Requirements Board (JFRB) for the GATES.

2.2. HQ AMC/A4TI will:

2.2.1. Serve as the Air Functional Manager for GATES and in this capacity will:

2.2.1.1. Coordinate with both internal and external program managers of automated information systems pertaining to the exchange of information between their systems and GATES.

2.2.1.2. Develop and review concepts of operation (CONOPS) for automation systems based on user requirements, higher headquarters directives, and new capabilities resulting from improved technology.

2.2.1.3. Manage GATES access requests.

2.2.1.4. Substantiate data systems development and implementation schedules.

2.2.1.5. Develop and/or validate Baseline Change Requests (BCRs), Software Problem Reports (SPRs), and Document Problem Reports (DPRs) applicable to GATES.

2.2.1.6. Maintain close liaison with the GATES Program Management Office (PMO).

2.2.1.7. Maintain close liaison with the GATES System Management Office (SMO).

2.2.1.8. Maintain close liaison with the GATES developers.

2.2.1.9. Maintain close liaison with the GATES users and serve as their advocate to the GATES PMO, GATES SMO, and GATES developers.

2.2.1.10. Make all necessary arrangements to provide AMC GATES users for AMC GATES Customer Acceptance testing in the GATES Port Simulation Center (GPSC) and augment the GATES test bed as required.

2.2.1.11. Coordinate installation and removal of GATES/Remote GATES (RGATES)/Deployed GATES (DGATES).

2.2.1.12. Work trouble tickets assigned to the Functional Managers through C2Remedy.

2.2.1.13. Maintain the HQ AMC/A4TI web pages and ensure the functional information on the web pages is current.

2.2.2. Research and integrate new technologies into AMC transportation systems.

2.2.3. Serve as the AMC functional point of contact for issues concerning non-AMC transportation systems.

2.2.4. Serve as the Chairman of the Transportation Functional Management Board (FMB).

2.2.5. Serve as a voting member on the Transportation Configuration Control Board (CCB).

2.2.6. Ensure GATES requirements are included in air transportation submissions to joint strategic planning documents and the biennial planning, programming, and budgeting system.

2.2.7. Ensure the requirement for foreign national background investigations is included in all contract vehicles for services provided at air terminals and commercial gateways in locations where foreign nationals provide the services and must have access to GATES.

2.3. **Other HQ AMC/A4T Branches will:**

2.3.1. Notify A4TI of GATES related issues.

2.3.2. Submit and/or coordinate on BCRs, SPRs, and DPRs, as required.

2.3.3. Serve as a voting member on the Transportation FMB.

2.3.4. Work trouble tickets assigned to them through C2Remedy.

2.4. **HQ AMC/A4TR in addition will:**

2.4.1. Coordinate development and implementation of GATES training programs and material with USAF Expeditionary Center (EC).

2.4.2. Coordinate GATES user training issues with A4TI and USAF EC.

2.5. **HQ AMC/A4TC in addition will:**

2.5.1. Function as the approval authority for organizations requesting access to GATES for passenger bookings.

2.6. **The Chief, Programs and Integration Branch (HQ AMC/A6IM) will**:

2.6.1. Establish a GATES PMO and appoint a GATES Program Manager (PM).

2.6.2. Execute appropriate PMO responsibilities as articulated in DOD, Air Force, and AMC directives.

2.6.3. Secure funding for procurement, development, and implementation of hardware and software for AMC air terminals and aerial ports and non-AMC air terminals and aerial ports operated on AMC's behalf.

2.6.4. Provide GATES servers as required.

2.6.5. Function as the GATES point of contact related to Inmarsat satellite communications issues.

2.6.6. Manage all aspects of security for GATES including Workstation Area Security Officer (WASO) account creation and management for the air side of GATES.

2.6.7. Serve as the Chairman of the Transportation CCB.

2.7. **The Director of Global Readiness, AMC 618 AOC (TACC)/XOP), will:**

2.7.1. Task deployable units with appropriate automation systems, support elements, and trained personnel.

2.7.2. Submit and/or coordinate on BCRs, SPRs, and DPRs, as required.

2.7.3. Serve as a voting member on the Transportation FMB.

2.8. **The Director of Global Channel Operations, AMC 618 AOC (TACC)/XOG), will:**

2.8.1. Review system metrics and identify to HQ AMC/A4TI problem areas that impact efficient operation of transportation automation systems.

2.8.2. Develop, submit, validate, test, and/or implement system software BCRs, SPRs, and DPRs as required.

2.8.3. Serve as a voting member on the Transportation FMB.

2.8.4. Participate in developing future transportation automation system requirements.

2.8.5. Provide routing IDs for approved passenger booking agencies.

2.9. **375th Communications Group will:**

2.9.1. Establish a GATES SMO and appoint a GATES System Manager

2.9.2. Provide automated transportation systems sustainment and support services.

2.9.3. Ensure appropriate documentation, technical library, and software/equipment user's manuals are current and changes are released to the field.

2.9.4. Obtain transportation policy and technical information from HQ AMC/A4T to support the sustainment of data management systems.

2.9.5. Coordinate with HQ AMC/A4TI in exercising technical operation direction over resources for the purposes of maintenance in support of transportation automation systems.

2.9.6. Coordinate the release of system advisory notices, letters, messages, and software releases or updates with HQ AMC/A4TI.

2.9.7. Identify operational trends and recommend improvements to the GATES PMO and HQ AMC/A4TI.

2.9.8. Maintain a 24/7 customer support branch (help desk) for operational problems or system outages.

2.9.9. Maintain working documents to track network and systems problems and make available to update HQ AMC/A4TI as requested.

2.9.10. Maintain the GPSC, ensuring it is operational and stable a minimum of two weeks prior to any scheduled functional software testing.

2.10. **Aerial port squadrons and air terminals operated on AMC's behalf will:**

2.10.1. Develop and submit system software BCRs and DPRs as required.

2.10.2. Participate in developing future transportation automation system requirements.

2.10.3. Configure and install GATES-related devices to support transportation automation in the air terminal.

2.10.4. Maintain local area network.

2.10.5. Ensure adherence to the requirements of all applicable AMCI 24-101 Volumes.

2.10.6. Follow established GATES policies and operating instructions as identified in AMC instructions, the GATES Installation and Operations Documents (GIOD), GATES Certification and Accreditation (C&A) documentation, policy memorandums, and other such guidance as promulgated by HQ AMC.

2.10.7. Locally manage GATES equipment, to include maintaining accountability in accordance with applicable Air Force Instructions, according to the policy established by HQ AMC and ensure that the life cycle replacement hardware is installed in a timely manner.

2.10.8. Create a Trouble Ticket log and internal process to ensure all GATES related problems, to include Automatic Identification Technology (AIT), are tracked and fixed in a timely fashion.

2.11. **GATES parent sites will:**

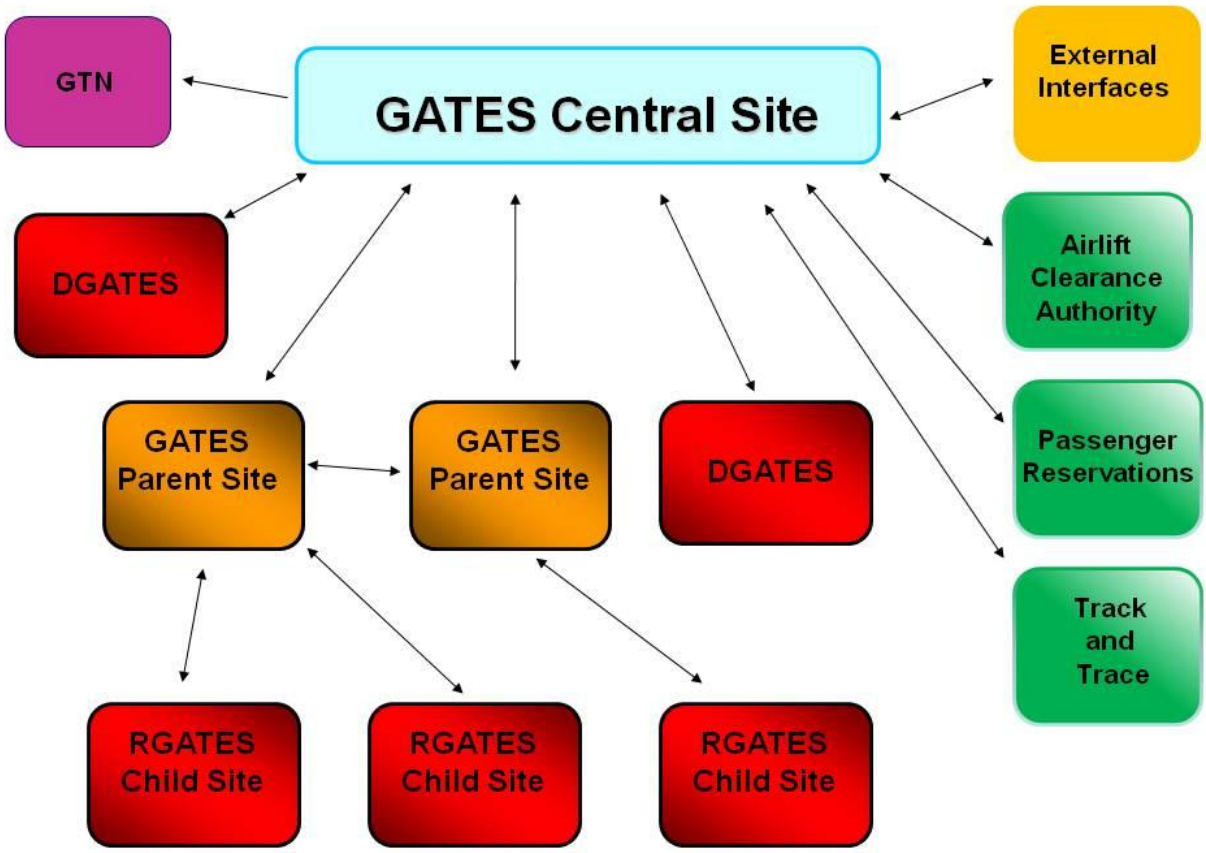
2.11.1. Assist as required with installation of RGATES servers at locations identified by HQ AMC/A4TI.

2.11.2. Train personnel at child sites on GATES operation, as required.

3. Transportation Systems

3.1. **GATES**. This is AMC's automated air transportation management system. GATES access requires a valid need-to-know, background investigation (National Agency Check with Inquiries (NAC-I) or Host Nation Equivalent), and annual computer based information assurance training. GATES issues a distinct user account when the above conditions are met. The individual's DOD issued Common Access Card (CAC) and digital certificates are used for authentication to the GATES system. GATES will continue to allow the use of passwords for authentication where required (e.g., handheld terminals (HHTs) without CAC readers), or until directed to discontinue their use by the directing authority. An important distinction to understand with the GATES architecture is that GATES is web-enabled and should not be considered web-based. While GATES is accessed via the Internet Explorer web browser, at those locations where cargo and passengers are manifested, a web server is physically located at each aerial port and the GATES user connects directly to that local web server. That web server then connects back to Central Site servers at Scott AFB. Only a few GATES users connect directly to the Central Servers at Scott AFB: Transportation Offices making passenger reservations, certain Air Clearance Authorities (ACAs), those using cargo Track and Trace, users of the GATES Enterprise Management Service (GEMS) and those accessing GATES from Scott AFB, i.e. HQ AMC or TACC users with GATES accounts or "ad hoc" query and reporting tools using a variety of Commercial-Off-The-Shelf (COTS) business intelligence applications. This explains why GATES cannot simply be fielded at any site that desires GATES access. Installation of servers and associated equipment is required in order to process cargo and passengers. Due to the expense and complexity, expansion of GATES to new locations is carefully controlled. Figure 1 provides an overview of the GATES connectivity architecture.

Figure 3.1. GATES Connectivity Diagram



Note: There are essentially six different types of GATES configurations as follows:

3.1.1. **GATES/RGATES.** This configuration is found at the larger, fixed location aerial ports where a large amount of transportation data is generated. A GATES/RGATES server is located at the site with access to the server via PCs using the local LAN. At a GATES site, the server connects to the rest of the GATES world by connectivity back to the central servers at Scott Air Force Base (AFB). At an RGATES site, the connectivity first goes through a parent GATES server and then back to the central servers at Scott AFB. See Figure 1 for a diagram of the GATES/RGATES connectivity.

3.1.2. **DGATES.** This is a transportable installation of GATES used to rapidly provide ITV in a deployed environment. These installations are managed as downward directed taskings by HQ AMC. A DGATES server is a ruggedized computer capable of working in austere environments. It connects directly back to the central servers at Scott AFB either via the site's LAN, using the computer's internal MODEM, or by satellite communications using Inmarsat/Broadband Global Area Network (BGAN). Often, a DGATES location does not generate large amounts of data, and if a local LAN is not available, the server does not have to be on line all the time. This is especially important when using communications where cost is determined by the amount of time connected, such as with the older Inmarsat satellite communications, rather than the amount of data transferred. Costs can be reduced by only connecting the DGATES computer when there

is data to transfer. The site can dial up through the satellite, allow replication to proceed with the central servers, and then disconnect the system. See Figure 1 for a diagram of the DGATES connectivity.

3.1.3. **Track and Trace.** Track and Trace provides essentially the same tracking capability found in the GATES/RGATES configuration, but doesn't require installation of equipment. The user simply uses a PC with a 128-bit encryption capable browser and connects to the GATES Track and Trace web site (**https://gatesea.gates.scott.af.mil**). Track and Trace is provided to personnel/organizations with a valid need to track cargo within the AMC airlift system. See Figure 1 for a diagram of the Track and Trace connectivity.

3.1.4. **Passenger Reservations.** Passenger Reservations, like Track and Trace, uses a web browser to connect to the GATES website (**https://gatesea.gates.scott.af.mil**). The function is limited to organizations authorized to make passenger reservations on AMC organic/charter aircraft. See Figure 1 for a diagram of the Passenger Reservation connectivity.

3.1.5. **Mini GATES.** Mini GATES is a subsystem of GATES and provides a limited web-based capability to process inbound and outbound cargo and passengers. This capability is made available to small, remote ports to provide in-transit visibility of cargo and passenger movement and facilitate prompt, accurate billing for the transportation services. All data must be manually entered, so it is not appropriate for larger aerial port operations. It was designed to be operated by personnel with minimal GATES experience.

3.1.6. **Airlift Clearance Authority (ACA).** ACA uses a web browser to connect to the GATES website (**https://gatesea.gates.scott.af.mil**). Airlift Clearance Authorities from the Air Force, Navy, Army, and Marine Corps use the ACA application to add, modify, and delete their particular service's advances in GATES. See Figure 1 for a diagram of the ACA connectivity.

3.1.7. **Other GATES Configurations and Equipment**

3.1.7.1. **Handheld Terminals (HHTs).** GATES takes advantage of automatic identification technology, to include bar-coded military shipping labels (MSLs), by the use of HHTs (also called bar code scanners) at aerial ports for cargo processing operations. GATES uses AIT devices to improve cargo processing accuracy and efficiency by allowing air transportation specialists to perform real-time updates to the system from the same location they are working the cargo/pallets. The user can in-check, inventory, palletize, manifest surface or air, along with every action required to manage cargo (e.g., split, consolidate, frustrate) all from the device inside or outside the warehouse. The HHTs utilize touch screen capability, linear and 2D bar code scanning, and real time access via Radio Frequency Data Communications (RFDC), or Wireless Local Area Network (WLAN) interactive connectivity, to the GATES data base. HHTs also provide non-interactive capability where RFDC coverage is intermittent or not available. The software on the HHT platform looks and feels like the GATES software since the HHT software was written to parallel that of GATES.

3.1.7.2. **Radio Frequency Identification (RFID).** To increase Total Asset Visibility (TAV) for the Combatant Commanders (COCOMs), the DOD directed the use of active RFID tags on cargo moving to, within, and from the COCOM's area of responsibility (AOR) through the Defense Transportation System (DTS), to include port-built air transportation pallets. In response to this tasking, RFID tag write capability was added to GATES. GATES obtains any available content level detail data directly from the Defense Logistics Agency E-Business Server upon in-check of cargo at an aerial port. GATES then allows writing both Transportation Control and Movement Document (TCMD) data and content level detail data to the active RFID tag during pallet Close and Process (CAP) procedures. GATES then sends the combined data to the Army's Radio Frequency (RF) ITV (RF-ITV) server. This provides the COCOMs a data-rich RFID tag allowing anyone with a Handheld Interrogator (HHI) to determine what requisitions are on the pallet. Also, during surface movements, the RFID-tagged pallet passes choke-point interrogators that relay movement information to the RF-ITV server. The server matches the RFID tag ID with the TCMD and requisition data for near-real time ITV and TAV to anyone with an account for the RF-ITV server.

3.1.7.3. **GATES Enterprise Management Services (GEMS).** GEMS is a query based tool that provides ports and other ITV users a capability to easily access both current and historical GATES data. Available as an assigned role to a regular GATES account, GEMS provides pre-formatted queries and allows for the development of additional queries based on new functional requirements. The information displayed by GEMS comes directly from either legacy databases, real time data from Central Site servers, or aerial port servers depending on what data is being requested.

3.1.7.4. **GATES Mobile Workstation (GMW).** The GMWs are designed to provide mobile GATES functionality within the warehouse or ramp environment. There are two configurations of the GMW: one is designed for mounting in a vehicle (GMW 1) and the other is mounted on a wheeled cart (GMW 2). The cart provides the following equipment; WLAN capable computer with Common Access Card (CAC) reader, keyboard, and optical mouse; 19 inch monitor; military shipping label printer with Universal Serial Bus (USB) cable; pallet placard LaserJet printer with USB cable; Savi RFID Tag Docking Station; handheld imager with 15 foot cable. The vehicle mounted configuration consists of a Universal RAM-mount vehicle assembly, a wireless tablet computer, and an inkjet printer with USB cable.

3.1.7.4.1. To fully capitalize on the capabilities of the GMWs, as well as the HHTs, wireless connections are required. The expectation is for GATES to run on the base wireless infrastructure instead of a dedicated GATES wireless network. Units need to submit a work order with the base communications organization requesting GATES hardware be part of the installation's wireless infrastructure. Inform HQ AMC/A4TI of any difficulty with obtaining wireless connections for GATES.

3.1.7.5. **Passenger Kiosks.** Provide a self-service center in each passenger terminal allowing passengers to perform a number of processing functions via a free standing passenger kiosk. Passengers interact with the kiosk via a touch screen. Capabilities

include, but are not limited to: allowing space-available/required (space-A/R) sign-up; allowing space-A/R passengers to mark/unmark themselves present; and allowing space-A/R passengers to check-in for a flight.

3.1.7.6. **Flight Information Display System (FIDS).** FIDS is used to provide passengers information about arriving flights, departing flights, and general information about the aerial port. All three of these components can be displayed on the same monitors in a revolving format or on separate monitors throughout the terminal.

3.1.7.7. **Printers.** GATES uses a variety of printers to provide necessary output documentation. These printers include: military shipment label printers, (e.g., desk top and portable shoulder- carried), baggage tag and boarding pass printers, and standard laser printers for printing reports, manifests, placards, etc.

3.1.7.8. **Data Processing Center (DPC) Server.** The DPC server is a GATES server that allows the AMC DPC to view all manifest registers and input manifest data as required for any aerial port worldwide. Only DPC personnel have access to this server. The server business rules allow manifesting data to stay active beyond the normal purge rules found on other GATES servers. This allows the DPC to make corrections to manifest discrepancies when aerial port personnel are not able to. Additionally, this server is capable of opening passenger flights beyond one hour after departure when other GATES servers are locked out. The DPC server is robust enough to handle all cargo and passenger transactions. Should an aerial port be forced to go to manual processing for a prolonged period of time, the capability exists to e-mail the data to the DPC where it can be entered into the GATES system as if from the originating APC. This provides for continuous ITV on the cargo and pax and allows processing by down line GATES stations without having to manually input the data themselves.

3.2. **Additional Transportation Systems.** In addition to GATES, there are other automated information systems which impact AMC transportation. There are many systems which interface GATES, but the following systems are ones with which an AMC transporter is most likely to interact with.

3.2.1. **Cargo Movement Operations System** (**CMOS).** CMOS is a combat support system that provides automated base level processing of cargo for movement during peacetime and deployment cargo and passenger movement during contingencies for the Air Expeditionary Forces. CMOS is the Air Force's designated deployment system for use at non-AMC locations as well as those AMC locations that do not have GATES.

3.2.2. **The Transportation Coordinators' – Automated Information for Movements System II (TC-AIMS II).** An Army system, TC-AIMS II provides an integrated information transportation system capability for routine deployment, sustainment, and redeployment/retrograde operations. TC-AIMS II automates the processes of planning, organizing, coordinating, and controlling unit-related deployments and sustainment. It also automates the day-to-day Installation Transportation Officer/Transportation Management Officer operations, redeployment and retrograde operations in support of the Defense Transportation System.

3.2.3. **Automated Air Load Planning System (AALPS).** AALPS is a knowledge-based system that assists users in the complex task of planning and execution of aircraft loads for all types of deployments. This entails the use of preplanned data (estimates) and actual data for both "real-world" and "What-if" scenarios. AALPS is used for estimating airlift requirements (by specific aircraft type and delivery method), producing USAF certified "flyable" load plans and providing airlift/movement summary data and load reports ranging from a single mission to full-scale division deployments. It was selected as the aircraft load planning system for the Department of Defense. AALPS is fielded to Army, Air Force, Navy, and Marine Corps units. Plans are being formulated to incorporate the capabilities of AALPS into SDDC's Integrated Computerized Deployment System (ICODES), making ICODES the DOD aircraft load planning system.

3.2.4. **Mechanized Materials Handling System (MMHS).** The new generation of MMHS is computerized and can remotely store and retrieve pallets. Since the MMHS requires much of the same information already in GATES (e.g., Transportation Control Numbers (TCNs) or pallet IDs), an interface between the MMHS and GATES was developed to share information. Due to security concerns, the initial MMHS installations do not have a direct interface with GATES. An intermediary computer is used which acts as the transfer device. The MMHS server transfers data to the intermediate computer where the GATES-MMHS client is running. The GATES-MMHS client then pushes the MMHS information to the GATES port server where it is processed. Responses to the MMHS data and new pallet data from the GATES port server are then prepared for transfer to the MMHS server. The GATES-MMHS client pulls the data from the GATES port server and places it in a directory on the intermediate computer where the MMHS server can then retrieve and process the data.

3.2.5. **Integrated Computerized Deployment System (ICODES)**. ICODES provides for a single, cross-service, planning and execution system for ship loading and stowage. It is engineered to provide users with intelligent decision-support during administrative, preposition, and humanitarian assistance operations. ICODES integrates multiple expert programs, knowledge bases, and graphical user interfaces within a computer-based distributed cooperative operational environment. ICODES was selected as the preferred migration system for shipload planning and will also incorporate the air load planning capabilities of AALPS.

3.2.6. **Integrated Data Environment (IDE)/Global Transportation Network (GTN) Convergence (IGC).** IGC provides DOD with an integrated set of networked, end-to-end visibility, deployment and distribution capabilities. IGC collects and integrates transportation information from selected transportation systems. The resulting information is provided to the SECDEF, Combatant Commanders, USTRANSCOM, its component commands, and other DOD customers to support transportation planning and decision-making during peace and war. The end goal of IGC is to effectively support the Joint Force Commander's ability to make decisions based on actionable logistics information.

3.2.7. **Deliberate and Crisis Action Planning and Execution Segments** (**DCAPES).** DCAPES supports USAF war planners and commanders in performing the tasks required to plan, source, mobilize, deploy, sustain, redeploy, and reconstitute forces for deliberate

and crisis operations. DCAPES produces two files for GATES. The first file contains data for passengers to be booked on a flight. The second file contains Unit Line Number (ULN) information. These files are imported into GATES via a manual, air gap interface.

4. GATES Procedures and Policies

4.1. Decommissioning RGATES/DGATES Servers.

4.1.1. **Procedures**. The following procedures have been developed to ensure all necessary actions are accomplished when an RGATES/DGATES site is decommissioned. If these steps are not accomplished, the server will not be ready to be deployed again and airlift manifests may remain in an un-reconciled status, thus preventing AMC from collecting airlift revenue. There are two distinct phases that must occur. The first concerns completion of the business rules associated with decommissioning a site while the second involves the actual decommissioning of the RGATES/DGATES server and return of the server to a deployable configuration. The business rules need to be accomplished before the server itself is decommissioned.

4.1.2. **Business Rules**

4.1.2.1. RGATES/DGATES sites must contact HQ AMC/A4TID Transportation Data Processing Center (DPC) (DSN 779-0045/Commercial (618) 229-0045 or e-mail to **AMC.A4TID@scott.af.mil**) not later than 5 days prior to decommissioning the servers/closing down locations, or as soon as possible in the case of a short notice site closure. The following information must be provided:

4.1.2.1.1. Name of the data records representative currently on station

4.1.2.1.2. Home station

4.1.2.1.3. Next station, if not classified

4.1.2.1.4. Incoming Contingency Response Group (CRG) representative or replacement unit

4.1.2.2. Personnel at RGATES/DGATES sites must provide information on the last passenger/cargo manifest number/reference generated at the five day point and follow up with a tentative list not later than twenty-four hours prior to departure with the last manifest references to be created for final mission departures. This will let the DPC know status prior to actual closure.

4.1.2.3. Personnel at RGATES/DGATES sites must provide the number of over/short (O/S) shipments and the status of shipments (Tracer Action or Transportation Discrepancy Report (TDR) action in progress).

4.1.2.4. Personnel at RGATES/DGATES sites must provide the DPC with any outstanding trouble ticket numbers and situations causing trouble ticket action, if required. (NOTE: This provides the DPC the ability and opportunity to compare what is left in the user system versus what can be seen in GATES_C.)

4.1.2.5. Clear all manifests prior to decommissioning of the site/server. There should be minimal fallout for the DPC to clear for departing units in the event processes cannot be completed due to trouble ticket action or assault departures. Forward all pertinent documentation to the DPC in these instances only. Otherwise, all

documentation will be sent to the appropriate staging facility upon departure, or as soon as possible thereafter.

4.1.3. **Server Decommissioning.** The procedures for decommissioning a DGATES server are found in the GIOD, Appendix V, *Deployable GATES Installation, Registration, and Notification*. The user should refer to the GIOD, which is available on the web by following the GATES Installation and Operations Documents (GIODs) link at URL https://www.my.af.mil/gcss-af/USAF/AFP40/d/1074111948/Files/a4t/a4ti/gates/hello.html to ensure the most current procedures are being followed. This action should only be performed if the DGATES location has completed the mission and the server needs to be cleaned and prepared for the next deployment. The server will not be decommissioned until all outstanding manifests are reconciled.

4.1.3.1. If a server is no longer going to be used as a GATES server, sanitation of all data from all storage devices that contained GATES data must be accomplished IAW AFSSI 5020 Remanence Security. GATES data contains sensitive government/DoD information as well as individual privacy act information and this data must be completely wiped from GATES systems once a server is no longer used for GATES applications.

4.2. GATES Change Control Process

4.2.1. **Change Mechanisms.** Three mechanisms exist where GATES users can make changes to the system and the GATES documentation. The three mechanisms are the BCR, SPR, and the DPR processes.

4.2.1.1. BCRs are used to make enhancements to the system or to change the way the system operates due to new or changing requirements. GATES users formulate an idea on how to improve GATES functionality and complete the BCR form. The form and instructions for completing the form can be found through the HQ AMC/A4TI web pages at URL **https://www.my.af.mil/gcss-af/USAF/AFP40/d/1074111948/Files/a4t/a4ti/gates/hello.html** and looking under the GATES Community of Practice (CoP) Homepage Links located in the left frame menu. When completed, the form is submitted to the GATES Functional Managers at HQ AMC/A4TI at Scott AFB, IL. Since any change to the GATES software takes time and funding, and must compete with other validated requirements, a formal BCR process has been established to ensure critical changes are addressed first. This process is described below in paragraph 4.2.2.

4.2.1.2. SPRs are used to correct deficiencies in the GATES software when the system is not operating as it should. The form and instructions for completing the form can be found through the HQ AMC/A4TI web pages at URL **https://www.my.af.mil/gcss-af/USAF/AFP40/d/1074111948/Files/a4t/a4ti/gates/hello.html** and looking under the GATES Community of Practice (CoP) Homepage Links located in the left frame menu. It should be noted that most SPRs result from a user reporting a problem to the help desk, and in the subsequent investigation of the trouble ticket, it is determined that a problem exists in the software. Rarely, if ever, will a user submit an SPR directly. In most cases, the developer will document the required fix action on the SPR and submit it to configuration management.

4.2.1.3. DPRs are used to correct errors in the GATES documentation, such as the GIOD or user manuals. If users find an error in the GATES documentation, the DPR should be completed. The form and instructions for completing the form can be found through the HQ AMC/A4TI web pages at URL **https://www.my.af.mil/gcss-af/USAF/AFP40/d/1074111948/Files/a4t/a4ti/gates/hello.html** and looking under the GATES Community of Practice (CoP) Homepage Links located in the left frame menu. When completed, the form is submitted to the GATES Functional Managers at HQ AMC/A4TI at Scott AFB, IL. The GATES Functional Managers will validate the DPR and submit to the GATES PMO for processing.

4.2.2. **GATES Software Change Process.** The time from BCR submission until the change is fielded can take up to a year and a half to accomplish. Many factors weigh into this process such as the complexity of the BCR, the priority the BCR is given, the point in the GATES release cycle that the BCR is submitted, as well as funding considerations. All have an impact on the length of time it takes a change to reach the field. The following is a description of the steps in the BCR process which every change must go through.

4.2.2.1. BCR submission. The BCR process is initiated when a user completes a BCR form and submits it to the GATES Functional Managers for consideration. In the Project Impact section of the BCR, clearly state what will happen if the requirement is not implemented or how much time and money will be saved if the change is approved. In addition, mention if the BCR is being written due to the result of a Lean initiative or Terminal 21 (T21) event. The BCR should also contain a few words on the submitter's expectations of what the change should accomplish. This is where the user states exactly what he/she expects to see or have GATES do when the change is implemented. This helps the software developer understand the intent of the requested change. Without this information, the BCR may not be adequately assessed by the headquarters air transportation functional community. The completed BCR can be mailed to HQ AMC/A4TI, 402 Scott Dr, Unit 2A2, Scott AFB, IL 62258-5308; faxed to DSN 576-1257 or commercial (618) 256-1257 or e-mailed to **AMC.A4TI@scott.af.mil.**

4.2.2.2. BCR processing. The GATES Functional Manager will review the submitted BCR, log it, and provide the other A4T branches a copy for their review. The branch which has responsibility for the BCR, e.g. A4TC will take ownership of cargo related BCRs, will ensure the BCR does not violate any established policies or business processes and perform a sanity check to ensure the BCR is a valid and necessary change. They will ensure the BCR is clearly written, and if necessary, contact the submitter for any required clarifications. Other branches will be provided a copy of the BCR to review and provide A4TI feedback as required. If the lead branch does not concur with the BCR, they will provide the GATES functional their rationale for non-concurring. The GATES functional will notify all the branches, as well as the submitter, that the BCR will not be processed and provide the rationale. BCRs can be disapproved for a number of reasons, e.g., it is a duplicate of another BCR, the change isn't necessary, the change is not possible, or the change violates established policy. If the lead branch concurs with the BCR, they will make any necessary modifications and return it to the GATES Functional to submit the BCR to

configuration management where it is assigned an official number. The GATES functional managers will then provide all the branches, as well as the BCR submitter, a copy of the final BCR so they may track its progress through the development cycle if desired.

4.2.2.3. BCR meets the GATES FMB. As the GATES budget is limited, it is important to take all the BCR submissions and rank them in priority order so the most important changes can be addressed first. The GATES FMB reviews all functional requirement BCRs to prioritize those affecting the user/functional communities. First the GATES Functional Managers analyze the BCRs prior to the FMB. An internal prioritization is accomplished and the prioritized list is then submitted to all branches within A4T. The formal FMB meets as required to discuss and finalize the priorities and this prioritized list is then submitted to the GATES CCB.

4.2.2.4. BCR meets the GATES CCB. The validated BCR is forwarded to the GATES CCB whose primary function is to manage the system baseline. The CCB is made up of the PM, System Manager (SM), the Functional Managers (FMs), Test Manager (TM), Configuration Manager (CM), and representatives such as Database Administrator (DBA), System Administrator (SA), Information/Protection/Security, Information Assurance Manager (IAM) Help Desk, and software engineers. The GATES CCB reviews and validates all new requirements and change requests to the existing GATES software and hardware baseline. The CCB works to prioritize developmental/ maintenance activity and change requests based upon system requirements and cost. In some cases, BCR implementation will be deferred because it's too late to incorporate the change into the next GATES software release or is deemed too costly to be accommodated by the GATES program budget at the present time. At the end of this process the BCRs are allocated to a GATES release. Since GATES also incorporates requirements of the Worldwide Port System and the Defense Courier Service, a Joint Functional Requirements Board (JFRB), chaired by the United States Transportation Command (USTRANSCOM), has been chartered to appeal and adjudicate competing functional requirements.

4.2.2.5. Develop Software/Create Release Documentation. The software project manager, in coordination with the functional manager, develops the software to enable the requested change to GATES. This process usually involves several discussions between the developer and the GATES functional mangers to clarify the requirement and ensure the change is effectively incorporated into the release. Documentation, such as software and user manuals, is also updated to reflect the change.

4.2.2.6. Testing. Once the software is developed, it is provided to the government for testing to ensure it functions according to the documented requirement. The software is independently tested via the Applications Infrastructural Systems Support (AISS) contract in the GPSC. When the software passes AISS testing, the GATES Functional Managers, supported by GATES users from the aerial ports, perform customer acceptance testing to ensure the software functions as required. Errors are documented, sent back to the developer for corrections, and the software is tested again. Once all applications work according to the requirement, the software is accepted.

4.2.2.7. Authorize Release for Fielding. Following successful testing, the submitter's idea will be incorporated into a GATES release and fielded for all GATES users worldwide. In most cases, this will occur at the time of the next version release of the GATES software which will incorporate the other approved BCRs as well.

4.3. **GATES Access Process.** The following procedures apply to air transportation access requests only. Customers requiring GATES for SDDC or DCS related missions must contact those functional communities for access. Access to GATES requires a legitimate need and requests must meet the criteria outlined in the following paragraphs. To request approval, the requester completes the appropriate GATES Access Request Letter Template which can be found on the A4TI web site at URL: **https://www.my.af.mil/gcss-af/USAF/AFP40/d/1074111948/Files/a4t/a4ti/gates/accessprocess/hello.html**. The following paragraphs provide specific details on obtaining access.

4.3.1. **Aerial Port GATES/RGATES**

4.3.1.1. GATES installation at an aerial port is significantly more complicated since the GATES application is web-enabled, not web-based. This distinction requires modification to the GATES infrastructure as a GATES web server is installed at aerial port locations. The user's Internet Explorer on his or her computer connects to the local server and not directly to the central servers at Scott AFB. This architecture was chosen to allow the port personnel to continue to operate if outside communications are cut off. Once communications are restored, the server automatically replicates data back to the central servers. Modifications to the GATES infrastructure may require the purchase and installation of servers; therefore, these requests must be fully justified.

4.3.1.2. AFI 10-403, *Deployment Planning and Execution,* and AFI 24-114, *Small Air Terminal Operations* require the use of CMOS for deployment of Air Force forces except at AMC strategic aerial ports where GATES may be used instead. Strategic aerial ports are identified in Defense Transportation Regulation 4500.9-R, Part III, Mobility, Appendix M. CMOS is the Air Force standard system for deployment. One of the primary purposes of GATES is for Transportation Working Capital Fund (TWCF) reimbursement on channel traffic. The cost of operating GATES is recouped through TWCF, so installation of GATES at non-TWCF generating locations will not normally be approved.

4.3.1.3. The request process for GATES/RGATES begins with the requester completing the appropriate GATES/RGATES Access Request Letter Template. Air Force organizations must coordinate with their Major Command's (MAJCOM) or higher headquarters' transportation division as well as HQ USAF/ILGD before submitting the letter to HQ AMC/A4TI. Without concurrence of both the MAJCOM and HQ USAF, the request will be denied. Non-Air Force organizations must work requests through their service major command and USTRANSCOM. GATES/RGATES will not be installed at non-Air Force locations without the approval of USTRANSCOM. If approved, the GATES Functional Managers will work with the GATES PMO and the affected sites to coordinate the installation of GATES/RGATES.

4.3.2. **Track and Trace.** Track and Trace request letters may be sent directly to HQ AMC/A4TI. Since IGC is the DOD approved system for ITV, requests for GATES Track and Trace must include a statement as to why IGC will not meet the requester's needs. If approved, the requester is sent an e-mail notifying them of the approval with the WASO appointment letter template attached. The requester fills in the required information and has the letter signed by the commander or equivalent, e.g. Division Chief, Operations Officer, Flight Commander, etc. This signature may be accomplished either by pen (preferred) or digitally with the CAC. A signed copy must be maintained at each site as a source document. Once signed, the appointed WASO sends the letter to the GATES System Security Office (SSO) at **208@scott.af.mil** attached to a digitally signed e-mail. The GATES SSO creates the WASO accounts and sends the new WASOs their login instructions. The new WASOs then create any additional track and trace accounts, to include replacement WASO accounts, required in their organization.

4.3.3. **Passenger Reservations.** Requests to gain access to GATES to make Passenger Reservations must be sent to HQ AMC/A4TI for consideration. The Defense Transportation Regulation (DTR) Part I, Passenger Movement, states it is DOD policy that official travel providers/Transportation Officers (TOs) will make AMC channel airlift seat reservations directly in the AMC passenger seat reservation system, GATES. Access to GATES to make passenger reservations will not be approved for any organization not designated as a transportation office or official travel provider. All other organizations must work through their local/supporting transportation officer for passenger reservation support. The request letter must include the activity's routing indicator or contain a statement that a routing ID needs to be assigned. AMC will assign a routing ID if the request is approved. AMC will staff the request within HQ AMC/A4T and, if approved, the requester is sent an e-mail notifying them of the approval with the WASO appointment letter template attached. The requester fills in the required information and has the letter signed by the commander or equivalent, e.g. Division Chief, Operations Officer, Flight Commander, etc. This signature may be accomplished either by pen (preferred) or digitally with the CAC. A signed copy must be maintained at each site as a source document. Once signed, the appointed WASO sends the letter to the GATES SSO at **208@scott.af.mil** attached to a digitally signed e-mail. The GATES SSO creates the WASO accounts and sends the new WASOs their login instructions. The new WASOs then create any additional passenger reservations accounts, to include replacement WASO accounts, required in their organization.

4.3.4. **GEMS.** Access to GEMS is via a regular GATES account with an associated GEMS role. If the requester's organization already has GATES or GEMS users, the person requiring GEMS should contact the unit's GATES WASO to obtain a GATES account with the GEMS role. If the requester is not at a location with a GATES WASO, they must submit the appropriate access request letter requesting GEMS directly to HQ AMC/A4TI. If approved, the requester is sent an e-mail notifying them of the approval with the WASO appointment letter template attached. The requester fills in the required information and has the letter signed by the commander or equivalent, e.g. Division Chief, Operations Officer, Flight Commander, etc. This signature may be accomplished either by pen (preferred) or digitally with the CAC. A signed copy must be maintained at each site as a source document. Once signed, the appointed WASO sends the letter to the

GATES SSO at **208@scott.af.mil** attached to a digitally signed e-mail. The GATES SSO creates the WASO accounts and sends the new WASOs their login instructions. The new WASOs then create any additional GEMS accounts, to include replacement WASO accounts, required in their organization.

4.3.4.1. GEMS accounts must be placed into the appropriate GEMS Group in order for the user to access the port data required and to also allow sharing of reports with other members of the same GEMS Group. At an aerial port, the GEMS user will normally be restricted to the data at his or her port. At other locations, e.g. Combatant Commands, MAJCOMS, Groups, Wings, etc, the GEMS user may be authorized access to more than one aerial port's data in order to retrieve data from all ports under their responsibility. When the WASO adds the GEMS role to a GATES user ID, the WASO can select the group the user ID belongs in. A WASO can only add a user ID to a group they themselves are in. New GEMS locations require creation of a new group which is accomplished in coordination with HQ AMC/A4TI during the initial request for GEMS access.

4.4. **WASO.** The WASO is responsible for managing GATES accounts at the site as well as ensuring GATES security issues are taken care of at his/her location. A GATES user with the sybase_acct_mgr role has full WASO privileges and is able to use most menu options of the GATES Security Services application. The sybase_acct_asst role only allows the WASO to lock, unlock, and reset user accounts. The two roles must never be assigned together. There is no limit to the number of WASOs allowed at a site, though, for effective account management, the sybase_acct_mgr role should be limited to a select few. As a general rule, at least one WASO must be available to reset accounts at all times. It is very important that the WASOs keep their e-mail addresses current within the GATES system as this is the primary method used by the GATES Functional Managers and GATES Security to contact them on GATES related issues. The e-mail address is easily updated using security services and the modify account option.

4.4.1. WASO Appointment Process.

4.4.1.1. Initial WASO appointment. WASOs must be appointed to the position. The initial WASO accounts at a new location are created by the GATES SSO. Personnel at the new location must obtain the WASO Appointment Letter Template from the GATES Informational Community of Practice (CoP) website. A link to the WASO Appointment Letter Template can be accessed at **https://www.my.af.mil/gcss-af/USAF/AFP40/d/1074111948/Files/a4t/a4ti/gates/hello.html**. Fill in the requested information and have it signed by the commander or equivalent, e.g. Division Chief, Operations Officer, Flight Commander, etc. This signature may be accomplished either by pen (preferred) or digitally with the CAC. A signed copy must be maintained at each site as a source document. Once signed, send the letter to the GATES SSO at **208@scott.af.mil** attached to a digitally signed e-mail. The GATES SSO creates the WASO accounts and sends the new WASOs their login instructions.

4.4.1.2. Subsequent WASO appointments. Once the GATES SSO has created the initial WASO accounts for a site, subsequent WASOs at the site are created locally. The commander or equivalent, e.g. Division Chief, Operations Officer, Flight Commander, etc., must sign the WASO appointment letter before the WASO adds the

WASO role (sybase_acct_mgr) to an existing account or creates a new user account with the WASO role. When existing WASOs no longer perform WASO duties, their WASO permissions/role must be removed. Only those users with the sybase_acct_mgr role are listed on the WASO appointment letter. Any time WASOs are added or deleted, a new WASO appointment letter is required to be signed and sent to the GATES SSO, via a digitally signed e-mail, to **208@scott.af.mil.**

4.4.2. User Account Management.

4.4.2.1. The WASOs (user with sybase_acct_mgr role) and assistant WASOs (user with sybase_acct_asst role) are the only users allowed access to the GATES Security Services application. WASOs can only create, modify, or delete user accounts at their location, e.g. a WASO at Dover AFB cannot accomplish account management for a user at Ramstein AB. Assistant WASOs can only reset user accounts. They cannot create or delete accounts. When a user no longer requires a GATES account, the account must be deleted within 24 hours after the user no longer requires access. The WASO needs to be notified when personnel leave the unit so this deletion can take place. WASOs should be on the unit's out processing checklist to ensure they are aware of personnel leaving the unit. GATES users ordered to a temporary duty location who have a requirement to use GATES at the new location must be assigned a Login ID at the new location. They may not use their home station GATES account when deployed. Home station WASOs will mark the TDY indicator for these users until they return to duty at home station.

4.4.2.2. Login IDs are auto generated from the user's name and then given a number from 00 to 99 that ensures individual accountability. System audits and GATES transaction audits track each action accomplished in GATES. A user account that a group of people share is not authorized as each user must only use their personal account to maintain accountability.

4.4.2.3. To be eligible for a GATES account, an individual must have as a minimum a favorable background investigation as well as documented information assurance training. Foreign nationals who require access to GATES in the performance of their duties are authorized a GATES account. They too require a favorable background investigation, i.e. National Agency Check or host nation equivalent and documented information assurance training. See paragraph 4.4.6. for specific procedures on providing foreign national access to GATES. User roles determine user permissions to access GATES information. As a rule, WASOs should assign the minimum number of roles required for the individual to accomplish his/her job. Refer to the GATES GIOD, Appendix P (see link in paragraph 4.6) for specific information concerning roles.

4.4.2.4. Every 30 days, the WASO will review account usage by printing a Delinquent User Account report from the GATES security services application. The WASO must contact delinquent users and determine if the user still requires GATES access. If access is no longer required, the WASO must delete the account. Any accounts showing 135 days of inactivity will be deleted automatically.

4.4.3. **Password Management**. Authentication to GATES for most users will be accomplished via the CAC. For a select few, e.g., those unable to obtain certificates or

possess equipment without CAC readers, user IDs and passwords are still an acceptable authentication method. When a new GATES user account is created with the Security Services application of GATES, a one-time use, 15 character password is established and time-expired 55 days. Users will only have 5 days to login using this one time password. Passwords expire every 60 days. User accounts are automatically disabled (locked) if the password expires. Most users will immediately link their user ID and password to their CAC when they first log in. Those users who still require a user ID and password for authentication will be linked to the P-Sync server where they will change their password and complete the password management process which will allow them to reset their own passwords in the future.

4.4.4. **User Revalidation**

4.4.4.1. GATES user accounts must be revalidated annually. This revalidation is a WASO responsibility and WASOs will be notified by GATES Security when the revalidation is due, normally in January. Sound security practices require user accounts to be deleted when a user no longer requires access to GATES. In many cases, the WASO is unaware of those individuals who no longer require access to GATES and the annual revalidation ensures that accounts no longer required are deleted. The WASO must contact each GATES user on the site user list report, determine if they still require GATES, verify the roles they have are the minimum required, and validate personal information, i.e. last name, first name and middle initial, rank, DSN phone #, e-mail address, type of security clearance, date of clearance, type of investigation, and citizenship. The WASO must meet each user face-to-face or if the user is geographically separated, the user must send the WASO a digitally signed e-mail containing the user's data to validate the user's identity. Accounts no longer required must be deleted.

4.4.4.2. WASOs must also complete new foreign national (FN) access requests for any foreign nationals still requiring GATES following the procedures in paragraph 4.4.6.

4.4.4.3. The WASO completes the user revalidation by selecting the User Revalidation application from the Security Services drop down window. The WASO should modify or delete accounts as required and accept those accounts that are required and up to date. The accepted accounts will then show as valid. Once valid, the WASO should select the "Send Revalidation Complete Message" from the activities drop down menu.

4.4.5. **GATES Server Patches.** Periodically, the GATES Security Auditors will scan a GATES server to determine if the server is up to date with the most recent security patches. If patches are missing, the site WASOs will be notified and provided a list of the patches required. It is a WASO responsibility to work with the local security/communications office to have the patches loaded onto the GATES server and notify GATES Security Auditors when finished. If the WASOs have any difficulty updating the server, the WASO must notify GATES Security Auditors for assistance.

4.4.6. **Foreign National Access to GATES.** Foreign Nationals (non-US citizens) have been authorized by the Air Mobility Command Vice-Commander to have access to GATES. The following procedures have been developed to ensure foreign nationals who

access GATES have a valid need-to-know and have been approved by the local commander to access the system.

4.4.6.1. Before granting access to GATES for any foreign national, the requirements of AFI 33-200 *Information Assurance (IA) Management*, AFI 31-501 *Personnel Security Program Management*, and AFSSI 8552 *Access to Information Systems* must be met. In summary, as a minimum, all foreign nationals must have a completed background investigation (National Agency Check with Inquiries (NACI) or host nation equivalent) and completed the annual Information Protection training. In addition, foreign nationals will be assigned the minimum number of roles required to accomplish their mission.

4.4.6.2. Commanders at the GATES site (O4 or higher) must authorize in writing foreign national access to GATES using the template available from the A4TI web pages at URL **https://www.my.af.mil/gcss-af/USAF/AFP40/d/1074111948/Files/a4t/a4ti/gates/hello.html**. Multiple foreign national users can be listed on the same document. This document requires signature (may be a digital signature) by the command authority (O4 or higher) at the GATES site. When signed, the WASO must e-mail these access requests, using a digitally signed e-mail, to GATES Security at **208@scott.af.mil.** The document will require annual update and forwarding to GATES Security. WASOs will not create any user IDs for foreign national personnel unless they have the signed letter from their commander authorizing them to do so.

4.4.6.3. Foreign national access to GATES will be revalidated during the annual GATES User Revalidation. Commanders will re-accomplish and sign a new foreign national GATES access letter for each foreign national requiring access to GATES. HQ AMC/A4T will periodically conduct a random audit of foreign national accounts to ensure compliance with these procedures.

4.4.7. **Physical Security.** The primary purpose of physical security is to prevent unauthorized access to equipment, facilities, material and information. Physical security includes physical barriers and control procedures. Physical security for GATES is provided by the entry control procedures of the facility where the equipment is housed and the application of standard resource protection measures. GATES equipment does not require any special physical security considerations beyond those specified in AFJI 31-102, *Physical Security* or AFSSI 8502 *Organizational Computer Security* for workstation security in the computing environment.

4.4.8. **Additional Information.** Detailed, information related to WASO responsibilities can be located on line through the HQ AMC/A4TI web pages at URL https://www.my.af.mil/gcss-af/USAF/AFP40/d/1074111948/Files/a4t/a4ti/gates/hello.html.

4.5. **GATES Training.** Air Force Air Transportation personnel receive GATES training at their technical training school at Ft. Lee, VA when they initially enter the career field. This training is an introduction to GATES only. In-depth training on GATES is provided at the aerial port via on-the-job training. As GATES is used by more than just Air Force Air Transportation specialists, additional training material has been developed to assist other users in becoming proficient in the use of GATES. A brief description of training material available is provided in the following paragraphs. All GATES training concerns should be addressed to HQ AMC/A4TR at DSN 779-4592.

4.5.1. **The Air Force Integrated Learning Center**. This organization has developed a web-based GATES training course. This course provides hands-on training to all users on using GATES to process passengers and cargo. The topics include outbound mission setup, cargo receipt and in-check, pallet processing, air and surface manifesting, passenger processing, and departing missions. A link to this training is available at **https://www.my.af.mil/gcss-af/USAF/AFP40/d/1074111948/Files/a4t/a4ti/gates/usermanuals/hello.html**. You must register for an account to take the course.

4.5.2. **On-line Training Servers.** AMC has developed on-line training servers to provide familiarization training on using GATES. Two servers are available; one for Passenger Reservations / Track and Trace functionality and one for aerial port functionality. These servers can be accessed at the AMC/A4TI web page at URL: **https://www.my.af.mil/gcss-af/USAF/AFP40/d/1074111948/Files/a4t/a4ti/gates/usermanuals/hello.html**. Instructions for using the training servers can be found by following the Training Server Instructions link.

4.5.3. **Stand-alone Training Server Software.** Interactive training capability is required for transporters that are not located at operational GATES sites, e.g. Guard and Reserve personnel, and therefore have no hands on training capability available to them. These individuals often deploy to locations with GATES and require a way to become familiar with the system. The stand alone training server software was developed to accommodate this requirement. Users are able to train on individual activities and units can conduct training scenarios that mirror normal port processes. The training server data base contains a snap shot of a real aerial port's data that can be manipulated. Users can also generate new missions and cargo/pax data. The software supports a minimum of four client computers connecting to another computer acting as a GATES server. Software is available at URL **https://www.my.af.mil/gcss-af/USAF/AFP40/d/1074111948/Files/a4t/a4ti/gates/usermanuals/hello.html**.

4.5.4. **Pamphlets.** Several training pamphlets are also available to provide familiarization on GATES operation and can be located on line through the HQ AMC/A4TI web pages at URL **https://www.my.af.mil/gcss-af/USAF/AFP40/d/1074111948/Files/a4t/a4ti/gates/usermanuals/hello.html**.

4.5.5. **DOD Information Awareness (IA) Training.** In accordance with Chairman Joint Chiefs of Staff Manual (CJCSM) 6510.01 all DOD military, civilian, and contractors will receive documented Information Awareness (IA) training prior to receiving access to the network. Training required to obtain a network user license is standardized in the "*Information Assurance Awareness Training"* Web-Based Training (WBT) course. Access the WBT on the current IA training site via the Air Force Portal. Successful completion of this course satisfies the Air Force training requirement for a network user license. Annual system security training is required IAW AFI 33-115 V2, *Licensing Network Users and Certifying Network Professionals*.

4.6. **GATES documentation.** Additional, detailed information related to GATES can be located on line through the HQ AMC/A4TI web pages at URL **https://www.my.af.mil/gcss-af/USAF/AFP40/d/1074111948/Files/a4t/a4ti/gates/hello.html**. The GATES User Manuals (GUMs), GIODs, WASO instructions, and other GATES related documentation can all be accessed through this link. These documents are important as they provide instruction on how your computer and/or internet browser need to be configured to work with GATES and also provide guidance on how to use the system.

4.7. **GATES Help Desk.** If a user experiences any problems with GATES, their first action should be to call the C2 Call Center at DSN 576-4949/Commercial 618-256-4949, Option 1 to reach the GATES Help Desk, or e-mail to **amctranshelpdesk@scott.af.mil.** The user can set the priority of the problem as either low, medium, high or critical. If the issue is causing a work stoppage, the user should inform the help desk. The GATES Help Desk will open a trouble ticket with the customer and pass the problem off to the appropriate agency for corrective action. Once corrected, the help desk will contact the submitter to determine if the issue was satisfactorily resolved prior to closing the ticket.

5. Prescribed and Adopted Forms

5.1. Adopted Forms: AF IMT 847, Recommendation for Change of Publication

5.2. Prescribed Forms: None

KENNETH D. MERCHANT, Major General, USAF
Director of Logistics

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DTR 4500.9-R, *Defense Transportation Regulation, Part I, Passenger Movement,* 23 November 2010

DTR 4500.9-R, *Defense Transportation Regulation, Part II, Cargo Movement,* 4 January 2011

DTR 4500.9-R, *Defense Transportation Regulation, Part III, Mobility,* 28 January 2010

DTR 4500.9-R, *Defense Transportation Regulation, Part IV, Personal Property,* 2 December 2010

DTR 4500.9-R, *Defense Transportation Regulation, Part V, Department of Defense Customs and Borders Clearance Policies and Procedures,* 21 January 2011

DTR 4500.9-R, *Defense Transportation Regulation, Part VI, Management and Control of Intermodal Containers and System 463-L Equipment,* 3 March 2011

DTR 4500.9-R, *Defense Transportation Regulation, Part VII, Human Remains Movement,* 18 September 2007

DOD 4515.13-R, *Air Transportation Eligibility,* 1 November 1994

AFI 33-324, *The Information Collections and Reports Management Program: Controlling Internal, Public, and Interagency Air Force Information Collections,* 1 June 2000

AFI 33-332, *Privacy Act Program,* 29 January 2004

AFMAN 33-363, Management of Records, 1 March 2008

AFI 33-364, *Records Disposition-Procedures and Responsibilities,* 22 December 2006

AFPD 24-1, *Personnel Movement,* 1 September 1995

AFPD24-2, *Preparation and Movement of Air Force Materiel,* 3 September 2003

AMCI 24-101 VoL 6, Transportation Documentation, Data Records and Reports, 5 August 2009

AMCI 24-101 VoL 9, *Air Terminal Operations Center*, 24 November 2009

AMCI 24-101, VoL 10, *Military Airlift Fleet Service,* 27 April 2009

AMCI 24-101 VoL 11, *Cargo and Mail Policy,* 7 April 2006

AMCI 24-101 VoL 14, *Military Airlift Passenger Service,* 2 October 2009

AMCI 24-101, VoL 22, *Training Requirements for Aerial Port Operations,* 22 August 2008

Abbreviations and Acronyms

2D—Two Dimensional

AALPS—Automated Air Load Planning System

AB—Air Base

AFB—Air Force Base

AFMAN—Air Force Manual

AFRC—Air Force Reserve Command

AISS—Applications Infrastructural Systems Support

AIT—Automatic Identification Technology

AMC—Air Mobility Command

AMCI—Air Mobility Command Instruction

ANG— Air National Guard

AOR—Area of Responsibility

BCR—Baseline Change Request

BGAN—Broadband Global Area Network

C2—Command and Control

CA—Central Analysis

CAC—Common Access Card

CAP—Close and Process

CCB—Configuration Control Board

CIO—Chief Information Officer

CMOS—Cargo Movement Operations System

COCOM—Combatant Commander

CONOPS—Concept of Operations

CPRP—Chief Information Officer (CIO) Program Review Process

CRAF—Civil Reserve Air Fleet

CRG—Contingency Response Group

DCAPES—Deliberate and Crisis Action Planning and Execution Segments

DCS—Defense Courier Service

DGATES—Deployable GATES

DOC—Designed Operational Capability

DOD—Department of Defense

DPC—Data Processing Center

DPR—Document Problem Report

DSS—Distribution Standard System

DTR—Defense Travel Regulation

DTS—Defense Transportation System

FIDS—Flight Information Display System

FM—Functional Manager

FMB—Functional Management Board

GATES—Global Air Transportation Execution System

GEMS—GATES Enterprise Management Services

GIOD—GATES Installation and Operations Document

GMW—GATES Mobile Workstation

GTN—Global Transportation Network

GUM—GATES User Manual

HDB—History Data Base

HHI—Hand Held Interrogator

HHT—Hand Held Terminal

HQ—Headquarters

ID—Identification

IDD—Interface Design Document

IGC—Integrated Data Environment (IDE)/Global Transportation Network (GTN) Convergence

IT/NSS—Information Technology/National Security System

ITV—In Transit Visibility

JFRB—Joint Functional Requirements Board

LAN—Local Area Network

MAJCOM—Major Command

MISCAP—Mission Capability

MMHS—Mechanized Material Handling System

MODEM—Modulator Demodulator

MSL—Military Shipping Label

O/S—Over/Short

OPlans—Operational Plans

OPR—Office of Primary Responsibility

OR—Operationally Reportable

PC—Personal Computer

PDO—Publishing Distribution Office

PM—Program Manager

PMO—Program Management Office

RF—Radio Frequency

RFDC—Radio Frequency Data Communications

RFID—Radio Frequency Identification

RGATES—Remote GATES

SDDC—Surface Deployment and Distribution Command

SIPRNet—Secret Internet Protocol Router Network

SM—System Manager

SMO— System Management Office

Space A/R—Space Available/Required

SPR—Softball Problem Report

SSO— System Security Office

SUM—Software Users Manual

TACC—Tanker Airlift Control Center

TAV—Total Asset Visibility

TC-AIMS II—Transportation Coordinators' – Automated Information for Movements System II

TCMD—Transportation Control and Movement Document

TCN—Transportation Control Number

TDR—Transportation Discrepancy Report

TM—Test Manager

TO—Transportation Officer

TWCF— Transportation Working Capital Fund

URL—Uniform Resource Locator

USB—Universal Serial Bus

UTC—Unit Type Code

WASO—Workstation Area Security Officer

WLAN—Wireless Local Area Network

WPS—Worldwide Port System

Terms

Aerial Port— An airfield that has been designated for the sustained air movement of personnel and materiel as well as an authorized port of entrance into or departure from the country where located.

Automatic Identification Technology (AIT)— The group of technologies consisting of bar codes, radio frequency identification tags, Common Access Cards, and biometrics, which, when interfaced to information systems, provide automatic identification.

Baseline Change Request (BCR)— BCRs are used to make enhancements to the system or to change the way the system operates due to new or changing requirements. The BCR form is filled out and submitted to the GATES Functional Managers at HQ AMC/A4TI at Scott AFB, IL. Since any change to the GATES software takes time and funding, and must compete with other validated requirements, a formal BCR process has been established to ensure critical changes are addressed first.

Broadband Global Area Network (BGAN)— BGAN is the Inmarsat broadband digital service and is used by DGATES computers for their connectivity requirements. Downlink speeds of high-end BGAN terminals are up to 492kb/s and upload speeds slightly lower at 300-400kb/s.

C2 Remedy— C2 Remedy is the tool used to track GATES trouble tickets and corrective actions. It provides the capability of managing, tracking, or monitoring problem ticket information, including creating problem resolution requests, searching for existing problem ticket data, generating reports, and creating macros. When a user experiences a problem with GATES and calls the GATES help desk, an entry is made in C2 Remedy and a trouble ticket is assigned.

Configuration Control Board (CCB)— The CCB is the mechanism used to prioritize competing GATES requirements to ensure the most critical can be satisfied in the resource constrained software development environment. Members of the CCB are the GATES functional managers, GATES security, the GATES system managers, and the GATES program management office. The CCB reviews requirements against known resources and develops a prioritized list of requirements that can be met in the next GATES release cycle.

Document Problem Report (DPR)— DPRs are used to correct errors in the GATES documentation, such as the GIOD or user manuals. If users find an error in the GATES documentation, the DPR should be completed and submitted to the GATES Functional Managers at HQ AMC/A4TI at Scott AFB, IL. The GATES Functional Managers will validate the DPR and submit to the GATES PMO for processing.

Functional Management Board (FMB)— The FMB is the mechanism used to prioritize GATES functional requirements. Unsatisfied requirements from the functional community are reviewed and prioritized before meeting the CCB. This way, the most critical functional requirements are clearly identified and won't be overlooked during the CCB negotiations. The FMB is chaired by AMC/A4TI and consists of members from every A4T branch, the TACC, and FM.

Inmarsat— Inmarsat is the corporation that owns the Inmarsat satellite-based communication system. The satellite constellation was previously known as International Maritime Satellite (INMARSAT), developed by an intergovernmental organization consortium in 1979 to provide global safety and other communications for the maritime community. In 1999 it was transformed into a private company, Inmarsat, and INMARSAT no longer is a term used to identify the satellites.

Joint Functional Requirements Board (JFRB)— GATES has become more than an aerial port management tool and now incorporates aerial port, water port, and Defense Courier Service

(DCS) functional requirements. Each functional community independently submits their requirements to the GATES PMO, which at times, will result in conflicting requirements or too many requirements to implement with the resources available. The JFRB was created to deconflict and prioritize these competing functional requirements. The JFRB is convened as required and is chaired by USTRANSCOM/J3 who has tie breaking authority and also represents the DCS functional community. The Surface Deployment and Distribution Command (SDDC), representing the water port functional community and AMC, representing the aerial port functional community are voting members.

Program Management Office (PMO)— The PMO manages system development and acquisition of system hardware. The PMO is responsible for budgeting and scheduling GATES development to meet the functional requirements as stated in BCRs and the Software Requirements Specifications.

Software Problem Report (SPR)— SPRs are used to correct deficiencies in the GATES software when the system is not operating as it should. Most SPRs result from a user reporting a problem to the GATES help desk, and in the subsequent investigation of the trouble ticket, it is determined that a problem exists in the software. Rarely, if ever, will a user submit an SPR directly. In most cases, the developer will document the required fix action on the SPR and submit it to configuration management. The SPR will then be allocated to a GATES release, the software fixed, and then implemented when the next GATES software is released worldwide.

System Management Office (SMO)— The SMO manages the day-to-day system operations of GATES. They are responsible for monitoring server operation, uploading required patches, upgrading the servers with new software versions, hardware installation, responding to system outages, and performing required repair actions.